

No. 1:13-cv-00328 (MCA) (SMV)

1

2. “Electronically Stored Information,” “ESI,” or “Data” means “electronically stored information” as that term is used in the Federal Rules of Civil Procedure and that does not exceed the scope of discovery defined in Fed. R. Civ. P. 26(b)(1).

3. “Non-reviewable media” means media that a Party cannot review (because, for example, necessary equipment is unavailable or the files contained on the media are corrupted), and that the other Party agrees to exclude from discovery as not reasonably accessible electronically stored information under Section B.

4. “Parties” means the parties to this litigation, including their employees and agents.

5. “Policy” means a regular practice at an entity that managers know about and expect to be carried out.

6. “Relevant,” when used to describe an electronic or hard copy document means any document that does not exceed the scope of discovery defined in Fed. R. Civ. P. 26(b)(1).

B. Preservation Not Required for Electronically Stored Information That Is Not Reasonably Accessible.

1. The Parties stipulate that the following categories of electronically stored information are not reasonably accessible for the purposes of Fed. R. Civ. P. 26(b)(2)(B), and the Parties need not preserve them:

a. Data stored in a backup system for the purpose of system recovery or information restoration, including but not limited to, disaster recovery backup tapes, continuity of operations systems, and data or system mirrors or shadows, if such data are routinely deleted or written over in accordance with an established routine system maintenance practice;

b. Non-reviewable media;

- c. Voicemail messages;
- d. Instant messages, such as messages sent on AOL Instant Messenger or Microsoft Communicator;
- e. Text messages, such as cell phone to cell phone SMS messages;
- f. Electronic mail sent to or from a personal digital assistant (“PDA”) or smartphone (e.g., BlackBerry) provided that a copy of such email is routinely saved elsewhere;
- g. All electronic data stored on a PDA or smartphone, such as calendar or contact data or notes, provided that a copy of such information is routinely saved elsewhere;
- h. Logs of calls made from cellular phones;
- i. Deleted computer files, whether fragmented or whole;
- j. Data stored in random access memory (“RAM”), cache memory, or in temporary or cache files, including internet history, web browser cache and cookie files, wherever located;
- k. Data stored on photocopiers, scanners, and fax machines;
- l. Server, system, or network logs; and
- m. Electronic data temporarily stored by scientific equipment or attached devices, provided that the data that is ordinarily preserved as part of a laboratory report is, in fact, preserved in its ordinary location and form; and
- n. Data stored on systems that are no longer in use today and that were no longer in use 2 years before the complaint was filed.

2. Notwithstanding subparagraph a. above, if on the date of this agreement either Party has a Policy that results in the routine preservation of any of the categories of information

identified in subparagraph a, such Party shall continue to preserve such information in accordance with its Policy.

C. **Discovery Procedure for Documents and ESI**

1. **Use of Relevant Documents During Litigation.** Notwithstanding any other provision of this Order, the Parties may take any of the following actions with respect to documents and ESI that are relevant for the purposes of Fed. R. Civ. P. 26:

a. The Parties may continue to work, in the ordinary course of business, on relevant documents that meet the definition of Draft in Part A. However, the Parties shall preserve Draft documents for discovery.

b. The Parties may move relevant documents or ESI into files or folders that adhere to an organizational scheme that was created before the complaint was filed in this matter. Nothing in this paragraph prevents the Parties from implementing an organizational scheme that applies only to relevant documents or ESI created after the complaint was filed in this matter.

c. The Parties may delete, overwrite, or wipe relevant ESI from devices that are being replaced, upgraded, reimaged, disposed of, or returned at the end of lease, provided that the potentially relevant ESI is first copied to a new location in a manner that preserves the data, including metadata, that will be produced pursuant to Paragraph C.4 of this order.

d. The Parties may copy data from one device to another, or from one location to another, provided that a copy of the relevant ESI remains accessible in the first location or the new copy is created in a manner that preserves the data, including metadata, that will be produced pursuant to Paragraph C.34 of this order.

e. The Parties may load relevant loose ESI, for example Word documents stored on a file system and not attached to an e-mail or other container file such as a .ZIP or

.RAR file, into a enterprise content management system, provided that: (1) the enterprise content management system captures all of the metadata fields that must be produced under this order and does not convert the format of the ESI in a way that makes it significantly less accessible; or (2) the Parties maintain a copy of the ESI in its native format and make their production from this native file collection.

f. The Parties may upgrade, patch, reprogram, or customize software that stores relevant data, even if such actions alter the way data is maintained, stored, or viewed.

g. The Parties may take any of the following actions with respect to data in a relevant database provided that it is part of the routine use of the database: input additional data; access data; update the software running the database; append new data; and modify existing data.

h. The Parties may edit or take down any relevant data on a publicly accessible internet site.

i. The Parties may compress, decompress, encrypt, or decrypt data subject to preservation in this matter provided that any data losses during such processes do not result in loss of the metadata required to be produced under this Order or significantly degrade the quality of the data.

j. The Parties may update social media sites, but may not take affirmative steps to delete relevant data posted before the filing of the Complaint.

2. Preservation Does Not Affect Discoverability or Claims of Privilege. By preserving documents or ESI for the purpose of this litigation, the Parties are not conceding that such material is discoverable, nor are they waiving any claim of privilege.

3. Other Preservation Obligations Not Affected. Nothing in this agreement shall affect any obligations of the Parties to preserve documents or information, such as pursuant to court order, administrative order, or statute, or in response to other anticipated litigation.

4. Procedures for Production: The following procedures apply to producing documents or ESI. Compliance with these procedures shall constitute compliance with Federal Rule of Civil Procedure 34(b)(2)(E).

a. Paper documents: Documents printed on paper may be produced for inspection or as paper copies, or may be scanned and produced on a CD-ROM, DVD-ROM, or external hard drive.

i. Documents printed on paper that are produced for inspection or as paper copies must be produced as they are kept in the ordinary course of business or must be organized and labeled to correspond to the categories in a request for production. The Parties will reach mutual agreement about the time and place for the review of documents produced for inspection, and for any further copying or production of those documents in a different format.

ii. Paper documents that are not produced for inspection or as paper copies, but are instead produced on disc shall be scanned as 300 dpi single-page TIFF files, using CCITT Group IV compression. Each page shall be branded with a unique Bates number, which shall not be an overlay of the image. Attachments to documents shall be assigned Bates numbers that run consecutively after the Bates numbers of the documents to which they are attached. The images shall be accompanied by: (1) an Opticon™ or IPRO® “cross reference file” which associates each Bates number with its corresponding single-page TIFF image file; and (2) a “text load file” containing Concordance® delimited text that will populate fields in a searchable flat database environment, containing one line for each document and each of the applicable fields as

described in Appendix A. For each document scanned from hardcopy or containing redactions, OCR text should also be produced as a .txt file. The name of the text file should be the same as the document's first page/Bates number, with a .txt extension (Example: [Prefix]00000001.txt). Nothing in this stipulation requires a Party to manually populate a metadata field in Appendix A (other than Custodian) if such fields cannot be extracted from a document;

b. Word, WordPerfect, and PDF documents will be converted to single-page TIFF images for each page and produced consistent with the specifications in subparagraph C.4.a.ii and Appendix A. Extracted text from each document, or OCR text from a document that contains redactions, should be produced as a .txt file. The name of the text file should be the same as the document's first page/Bates number, with a .txt extension (Example: [Prefix]00000001.txt).

c. Microsoft PowerPoint files will be processed and produced in the same manner as Word, WordPerfect, and PDF documents, except that the images shall be generated as full color, full page, JPEG images with one slide per page. Notes and other text that would not appear on the screen in the presentation view need not be shown on the JPEG images. The receiving party may, after reviewing the produced images, request the native files;

d. E-mail and attachments should be converted to single-page TIFF images and produced consistent with the specification in subparagraph C.4.a.ii, above, and Appendix A. Extracted text from each document, or OCR text from a document that contains redactions, should be produced as a .txt file. The name of the text file should be the same as the document's first page/Bates number, with a .txt extension (Example: [Prefix]00000001.txt). E-mail attachments shall be processed as though they were separate documents, and the text load file

shall include a field in which the producing Party shall identify, for each e-mail, the Bates range of any attachment;

e. Microsoft Excel files and other spreadsheets will be produced in native file format in a separate folder on the production media. The text load file shall contain a field that identifies the file name and the file path of the native file corresponding to each document. The Parties shall provide a placeholder TIFF image that has the text “File Produced Natively” and also a Bates number.

f. Digital photographs will be produced as full color image files at their original resolution with Bates numbers branded onto them. If additional data about the photographs is needed, the parties will meet and confer to determine how the photographs will be produced;

g. Embedded files shall be treated as though they were separate files, except that the text load file shall include a field in which the producing Party shall identify, for each document containing an embedded file, the Bates range of any such embedded file. This Bates range may be identified in the same field as the Bates range of an e-mail attachment.

h. Before any Party produces any other kinds of electronic data, including data from databases, CAD drawings, GIS data, videos, etc., the Parties will meet and confer to determine a reasonably useable form for the production.

i. Except as expressly stated otherwise above, TIFF images produced in this matter may be black-and-white images (no shades of gray). However, the receiving party has the option, after reviewing the produced TIFF image, to enquire whether the original document contained color and, if so, to request a color image.

j. Except as stated above, a Party need not produce the same electronically stored information in more than one form.

5. Duplicates.

a. *Deduplication of e-mail.* The Parties shall identify exact duplicates of e-mails based on one of the following methods, and shall produce only one copy from each set of exact duplicates:

- i. comparing the MessageID or UNID metadata fields; or
- ii. calculating and comparing the MD5 or SHA-1 hash value.

b. The Parties hereby stipulate and agree that there shall be in this matter a rebuttable presumption of evidence that an e-mail correctly addressed to a recipient was actually delivered to that recipient's e-mail inbox.

c. *Deduplication of ESI other than e-mail.* The Parties shall identify exact duplicates of electronic files other than e-mail and attachments based on MD5 or SHA-1 hash values and shall produce only one copy of each file.

6. Meet and Confer Requirements.

a. *Extension of Time to File Motion to Compel.* Due to the significant volume of documents which will be at issue in the case, the parties will be unable to ascertain whether there are disputes regarding discovery within the 21 day time limitation for filing a motion to compel imposed by D.N.M. LR-Civ. 26.6. On account of this, and to avoid the parties having to file multiple motions for extensions of that 21 day time limitation, the parties shall be permitted to file a motion to compel within forty-five (45) days of the receipt of the other party's responses and objections to discovery or within forty-five (45) days of the production or inspection of documents produced in response to a discovery request, whichever is longer.

b. *Discovery Disputes.* Before filing any motion with the Court regarding electronic discovery or evidence, the Parties will meet and confer in a good faith attempt to resolve such disputes.

c. *Search Terms and Parameters.* The Parties will meet and confer to identify mutually agreeable search terms for email messages and other electronically stored information, however, this agreement to meet and confer does not obligate any Party to agree to perform an electronic search.

d. *Third-Party Data.* The Parties will meet and confer before serving any subpoenas in this matter on commercial e-mail providers, such as Google™ or Yahoo™, or any social media companies such as Facebook™ or Twitter™.

D. **Limitations on Discovery.**

1. No Discovery of Material Not Required To Be Preserved. The Parties shall not seek discovery of items that need not be preserved pursuant to paragraphs B.1 above. If any discovery request is susceptible of a construction that calls for the production of items that need not be preserved pursuant to paragraphs B.1, such items need not be searched for, produced, or identified on a privilege log pursuant to Fed. R. Civ. P. 26(b)(5).

2. Privileged Materials Located in the Offices of Counsel. The Parties agree that, in response to general discovery requests, the Parties need not search for and produce, nor create a privilege log for, any privileged or work product material that is located in the offices of the U.S. Department of Justice or outside counsel for Plaintiff Chevron Mining Inc, or any documents described in Section F.1 of this Order. But the Parties agree that they are obligated to disclose non-privileged, non-work product, factual information in any such documents in response to interrogatories or requests for admission.

E. **Protection of Privileges.**

Pursuant to Rules 16(b) and 26(c) of the Federal Rules of Civil Procedure, and pursuant to Rule 502 of the Federal Rules of Evidence, it is hereby ORDERED:

1. This Order invokes the protections afforded by Rule 502(d) of the Federal Rules of Evidence. Accordingly, the provisions in Rule 502(b) will not apply to the disclosure of communications or information in discovery in this matter.

2. The prosecution and defense of this action will require each Party to review and to disclose large quantities of information and documents, including electronically stored information, through the discovery process. As a result, page-by-page preproduction privilege review would likely impose an undue burden on the Parties' resources.

3. Each party is entitled to decide the appropriate degree of care to exercise in reviewing materials for privilege, taking into account the volume and sensitivity of the materials, the demands of the litigation, and the resources that the party can make available, including attorney review of selected documents and electronic keyword searches. Irrespective of the care that is actually exercised in reviewing materials for privilege, the Court hereby orders pursuant to Rule 502(d) of the Federal Rules of Evidence that disclosure of privileged or protected information or documents in connection with this litigation will not constitute or be deemed a waiver or forfeiture—in this or any other federal or state proceeding—of any claims of attorney-client privilege or work product protection that the disclosing Party would otherwise be entitled to assert with respect to the information or documents and their subject matter.

4. The Court further orders that because expedited or truncated privilege review is likely necessary for the just, speedy, and inexpensive resolution of this matter, and because Rule 502(d) does not preserve privileges other than the attorney-client privilege and work-product

protection, the disclosure of any privileged or protected information or documents in discovery conducted in this litigation will be deemed unintentional and inadvertent under this Court order. Such disclosure will not constitute a waiver of the disclosing party's right to claim any privilege or protection that would have applied to the information or documents or their subject matter but for the disclosure, provided only that the party disclaiming waiver employed procedures reasonably designed to screen out privileged materials. The Parties shall not argue, in this forum or any other, that any privileges or protections were waived as a result of disclosures in this litigation irrespective of the procedures used to screen out privileged materials.

5. If a Party determines that it has produced a document upon which it wishes to make a claim of privilege or work product protection, the producing Party shall, within 14 days of making such determination, give all counsel of record notice of the claim of privilege or work product protection. The notice shall identify each such document and the date it was produced. If the producing Party claims that only a portion of a document is privileged or protected, the producing Party shall provide, along with the notice of the claim of privilege, a new copy of the document with the allegedly privileged or protected portions redacted. Any party that complies with this paragraph will be deemed to have taken reasonable steps to rectify disclosures of privileged or protected information or materials.

6. If a Party identifies a document that appears on its face or in light of facts known to the Party to be subject to another Party's claim of privilege or work product protection, the Party identifying the potential claim of privilege or work product protection is under a good-faith obligation to notify the Party holding the potential claim of privilege or protection. Such notification shall not waive the identifying Party's ability to subsequently challenge any assertion of privilege or protection with respect to the identified document. If the Party holding the

potential claim of privilege or protection wishes to assert a claim of privilege or protection, it shall provide notice in accordance with paragraph 5 above within ten business days of receiving notice from the identifying Party.

7. To the extent that any Party obtains through disclosure any information, documents, or communications that appear to be subject to another Party's claim of privilege or work product protection, such information, documents, and communications shall not be filed or presented for admission into evidence or sought in discovery by that Party in *CMI v. United States*, Civil Action No. 1:13-cv-00328 (MCA) (ACT) (D.N.M.), or any other proceeding, except as provided in paragraph 9.

8. Upon receiving notice of a claim of privilege or work product protection on a produced document, the receiving Party must, in accordance with Fed. R. Civ. P. 26(b)(5)(B), promptly return or destroy the specified information and any copies it has and may not use or disclose the information. Copies of privileged or protected documents or information that have been stored on electronic media that is not reasonably accessible, such as disaster recovery backup media, need not be destroyed as long as they are not restored; if such data is restored, the receiving Party must take steps to destroy the restored information. If the receiving Party disclosed the information before being notified, it must take reasonable steps to prevent further use of such information until the claim is resolved.

9. If a Party wishes to dispute a claim of privilege or protection asserted under this Order, such Party shall, within 14 days, move the Court for an order compelling disclosure of the information, after fulfilling any meet and confer obligations as defined in Part C.6.a of this Order. The Party shall follow the procedures described in Fed. R. Civ. P. 26(b)(5)(B) and must not assert, as a ground for compelling disclosure, the fact or circumstances of the disclosure.

10. The Parties may stipulate to extend the time periods specified in paragraphs 5, 6, and 9 above.

11. Nothing in this order overrides any attorney's ethical responsibilities to refrain from examining or disclosing materials that the attorney knows or reasonably should know to be privileged or protected and to inform the disclosing party that such materials have been produced.

12. The Party wishing to assert a claim of privilege or work product protection retains the burden, upon challenge pursuant to paragraph 9, of establishing the applicability of the claimed privilege or protection by a preponderance of the evidence.

13. This Order does not preclude a Party from voluntarily waiving any claims of privilege or protection. The provisions of Rule 502(a) of the Federal Rules of Evidence apply when a Party uses privileged or protected information to support a claim or defense.

F. Preparation of Privilege Log.

1. The obligation to provide a log of privileged or work product materials pursuant to Rule 26(b)(5)(A) presumptively shall not apply to:

- a. Communications exclusively between a party and its counsel;
- b. All work product created by counsel, or by an agent of counsel other than a party or an employee of a party;
- c. All privileged materials created by counsel, or by an agent of counsel other than a party or an employee of a party after April 5, 2013; or
- d. Internal communications within (a) a law firm, (b) a legal assistance organization, (c) a governmental law office, or (d) a legal department of a corporation or another organization.

2. Embedded e-mails. An e-mail shall be treated as a single document regardless of the number of embedded emails contained within the message body. The privilege log for an e-mail withheld under a claim of privilege, to the extent any is required, shall identify the author, recipient(s), subject, dates and times based on the metadata from the top-level message, and shall not include data from any e-mail embedded in the message body. However, if an e-mail contains both privileged and non-privileged communications, the non-privileged communications must be produced. This requirement should be satisfied by producing the original of the embedded, non-privileged e-mail, but if the original is not available, it may be satisfied by producing a redacted version of the privileged e-mail.

G. Costs of Document Production. Unless this Court orders otherwise for good cause shown, each Party shall bear the costs of producing its own documents.

H. Expert Discovery.

1. Each Party shall not pursue through discovery, trial subpoena or otherwise:
 - a. Notes taken by a witness required to provide a report under Fed. R. Civ. P. 26(a)(2)(B);
 - b. Communications between a witness required to provide a report under Fed. R. Civ. P. 26(a)(2)(B) and a Party's representative—including, but not limited to, another witness required to provide a report under Fed. R. Civ. P. 26(a)(2)(B)—regardless of the form of the communications, except to the extent that the communications:
 - i. Relate to compensation for an expert's study or testimony;
 - ii. Identify facts or data that a Party provided and that the expert considered in forming the opinions to be expressed; or

iii. Identify assumptions that a Party provided and that the expert relied upon in forming the opinions to be expressed.

2. The Parties shall bear the costs of their own testifying experts in responding to discovery, and shall not require the Party seeking discovery to pay the other Party's testifying expert any fee for the time spent in responding to discovery.

I. **Integration/Appendices.** The following documents are incorporated herein by reference:

"Appendix A" is a table describing the fields to be included in the databases produced by each Party.

SO ORDERED this 6th day of February, 2014,



HON. STEPHAN M. VIDMAR
U.S. Magistrate Judge

Appendix A:
Fields to Exchange in Databases of Discovery Materials

Name of Field	Type of field	Contents				
		E-mail	Word Processing or PDFs	Spreadsheets	Digital Photos	Paper
Prod_Begin	Text	Bates number for the TIFF image of the first page	Bates number for the TIFF image of the first page	Bates number for the TIFF image of the first page, or, if spreadsheets are not TIFFed, the Bates number of the placeholder page	Bates number branded onto a TIFF file that has the same resolution as the native image file.	Bates number for the TIFF image of the first page
Prod_End	Text	Bates number for the TIFF image of the last page	Bates number for the TIFF image of the last page	Bates number for the TIFF image of the last page or, if spreadsheets are not TIFFed, the Bates number of the placeholder page	Bates number branded onto the native image file	Bates number for the TIFF image of the last page
Prod_Attachment_Range	Text	Bates range of the attachments. Only the first page of the first attachment and the last page of the last attachment are indicated.	Bates range of all embedded files and all documents (including e-mails) to which this file was attached or in which it was embedded. Only the first page of the first attachment and the last page of the last attachment are indicated.	Bates range of all embedded files and all documents (including e-mails) to which this file was attached or in which it was embedded. Only the first page of the first attachment and the last page of the last attachment are indicated.	Bates range of all documents (including e-mails) to which this file was attached or in which it was embedded. Only the first page of the first attachment and the last page of the last attachment are indicated.	
Custodian	Text	The name of the person who had primary control over the location from which the document was collected	The name of the person who had primary control over the location from which the document	The name of the person who had primary control over the location from which the document	The name of the person who had primary control over the location from which the document	The name of the person maintaining the file from which the paper was obtained
Author	Paragraph	"From" field	<blank>	<blank>	<blank>	<blank>

Name of Field	Type of field	Contents				
		E-mail	Word Processing or PDFs	Spreadsheets	Digital Photos	Paper
To	Paragraph	"To" field	<blank>	<blank>	<blank>	<blank>
CC	Paragraph	"CC" field	<blank>	<blank>	<blank>	<blank>
BCC	Paragraph	"BCC" field	<blank>	<blank>	<blank>	<blank>
Subject	Paragraph	"Subject" field	<blank>	<blank>	<blank>	<blank>
DateSent	Date	The date and time the message was sent	<blank>	<blank>	<blank>	<blank>
Message_ID	Text	For e-mails in Microsoft Outlook, the "Message ID" field; For e-mail stored in Lotus Notes, the UNID field	<blank>	<blank>	<blank>	<blank>
Filename	Paragraph	<blank>	The name the file	The name the file	The name the file	<blank>
Folder	Paragraph	<blank>	The complete file path for the location from which the file was collected, starting with the identification of the machine	The complete file path for the location from which the file was collected, starting with the identification of the machine	The complete file path for the location from which the file was collected, starting with the identification of the machine	<blank>
Native_File	Paragraph	<blank>	The path to the native file on the production media	The path to the native file on the production media	<blank>	<blank>
Textlink	Text	The path to the extracted text file with the following format: \TEXT\[Prefix][Bates number].txt.	The path to the extracted text file with the following format: \TEXT\[Prefix][Bates number].txt .	The path to the extracted text file with the following format: \TEXT\[Prefix][Bates number].txt .	<blank>	The path to the extracted text file with the following format: \TEXT\[Prefix][Bates number].txt .
MD5Hash	Text	MD5Hash value	MD5Hash value	MD5Hash value	MD5Hash value	<blank>